



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/839,300	04/23/2001	Yuefeng Liu	6502.0333	3107
22852	7590	02/08/2006	EXAMINER	
FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP 901 NEW YORK AVENUE, NW WASHINGTON, DC 20001-4413			NGUYEN, PHUONGCHAU BA	
			ART UNIT	PAPER NUMBER
			2665	

DATE MAILED: 02/08/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

6/2

Office Action Summary	Application No.	Applicant(s)	
	09/839,300	LIU, YUEFENG	
	Examiner	Art Unit	
	Phuongchau Ba Nguyen	2665	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 07 November 2005.
 2a) This action is FINAL. 2b) This action is non-final.
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 1-37 is/are pending in the application.
 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
 5) Claim(s) _____ is/are allowed.
 6) Claim(s) 1-37 is/are rejected.
 7) Claim(s) _____ is/are objected to.
 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.
 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) <input type="checkbox"/> Notice of References Cited (PTO-892)	4) <input type="checkbox"/> Interview Summary (PTO-413)
2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)	Paper No(s)/Mail Date. _____ .
3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date <u>1-19-6</u> .	5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)
	6) <input type="checkbox"/> Other: _____ .

Claim Rejections – 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

2. Claims 1–37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Arrow (6,175,917) in view of Giniger (6,751,729).

Regarding claim 1, Arrow (6,175,917) discloses A Method and Apparatus for Swapping A Computer Operating System. In Arrow, a *method for communicating between a first private network (LAN 110-fig.1) and a second private network (a VPN group including VPN units 115, 125, 135, 145, 155-fig.1, col.2, lines 22-27) configured from nodes (VPN units, fig.1) in a public network (public network 100-fig.1), comprising:*

receiving (receiving at VPN unit 115-fig.1) a packet from a source node (node 112-fig.1) in the first private network (LAN 110-fig.1), (see column 7, lines 20-25); determining (by the VPN unit 115-fig.1) whether the packet (from node 112-fig.1) is destined for the second private network (in the VPN group, fig.1), (see column 7, lines 28-48).

Arrow does disclose *forwarding the packet over a channel to a destination node* (remote client 140 of the VPN unit 145 -fig.1, Arrow) *in the second private network* (of the VPN group, see step 22-fig.2, Arrow) *based on the determination* (see column 8, lines 18-19, Arrow), except acquiring a channel key associated with a channel base on the determination, *wherein the channel comprises a plurality of virtual links through the public network that connects a plurality of channel nodes, the channel nodes including the source node and the destination node, such that only the channel nodes are permitted to communicate over the channel*, wherein the channel key is updated for a modification of the channel nodes

Arrow does explicitly disclose *forwarding the packet over a channel to a destination node* (remote client 140 of the VPN unit 145 -fig.1, Arrow) *in the second private network* (of the VPN group, see step 22-fig.2, Arrow) *based on the determination* (see column 8, lines 18-19, Arrow).

However, in the same field of endeavor, Giniger discloses *forwarding the packet over a channel* (secured tunneling) *to a destination node* (device 120-fig.1) *in the second private network* (VPN group, see col.7, lines 59-61) *based on the determination by obtaining an address mapping corresponding to a destination node in the second network* (see column 7, lines 54-64), *and acquiring a channel key associated with a channel based on the determination* (col.8, lines 28-42) *wherein the channel comprises a plurality of virtual links* (115-fig.1) *through the public network that connects a plurality of channel nodes, the channel nodes including the source node and the destination*

node, such that only the channel nodes are permitted to communicate over the channel, wherein the channel key is updated for modification of the channel nodes (col.7, lines 44-67).

Therefore, it would have been obvious to an artisan to apply Giniger's teaching to Arrow's system with the motivation being to provide a secured data transmission between nodes over Internet and to prevent unauthenticated entering the VPN.

Regarding claim 2, Arrow further discloses that *said forwarding comprising:*

(1) sending the packet to the destination node using the address mapping, the address mapping reflecting a relationship between (a) an internal address for the destination node for use in communicating among nodes in the second private network and (b) an external address for the destination node suitable for communicating over the public network.

Arrow further discloses the VPN unit 115-fig.1 sending a received data packet to the VPN unit 145-fig.1 using the LUR, see column 7, line 46-column 8, line 20 (corresponding to (1)). The LUR reflects a relationship between an internal address for the destination node VPN unit 145-fig.1 in the Virtual Private Network for communication among the VPN units, see column 7, lines 28-32 (corresponding to (a)), and an external address for the destination node VPN unit 145-fig.1 for communication over the public network, see column 7, lines 28-32 (corresponding to (b)).

Regarding claim 3, Arrow discloses when the data packet sending from an end-station 112-fig.1 to a router 114-fig.1, the packet is encapsulated (corresponding to *adding external address*) for transmission to a destination node 140 in the VPN unit 145-fig.1 in the public network 100-fig.1 through the VPN unit 115, see column 7, lines 20-25.

Regarding claim 4, Arrow further discloses the VPN unit 115-fig.1 *encrypting the packet* in sending process from a source address 112-fig.1 to a destination address 140-fig.1 of VPN unit 145-fig.1 in the VPN, see column 7, lines 57-60.

Regarding claim 5, Arrow further discloses the VPN unit 115-fig.1 accessing the LUR of the transmitting packet from the Lookup Tables. This LUR should correspond to a destination of the VPN unit 145-fig.1, see column 7, lines 28-32, also see claim 2, (corresponding to *accessing the address mapping based on a determination that the packet is destined for the second private network*).

Regarding claim 6, Arrow further discloses the VPN unit 115-fig.1 accessing the Lookup Tables to obtain a LUR for a destination address in the transmitting packet. This LUR identifies the existence of a member of individual VPN, which corresponds to the destination 140-fig.1 via the VPN unit 145-fig.1, see column 7, lines 28-32, 50-52,

also see claim 2, (corresponding to *determining whether an address mapping exists for a destination address in the packet*).

Regarding claim 7, Arrow discloses A Method and Apparatus for Swapping A Computer Operating System. In Arrow, a *method for communicating between a first private network (LAN 110-fig.1) and a second private network (a VPN group including VPN units 115, 125, 135, 145, 155-fig.1, col.2, lines 22-27) configured from nodes (VPN units, fig.1) in a public network (public network 100-fig.1), comprising:*

receiving (receiving at VPN unit 115-fig.1) a packet from a source node (node 112-fig.1) in the first private network (LAN 110-fig.1), (see column 7, lines 20-25);

determining (by the VPN unit 115-fig.1) whether the packet (from node 112-fig.1) is destined for the second private network (in the VPN group, fig.1), (see column 7, lines 28-48);

(1a) obtaining an address mapping corresponding to the destination node based on the determination and (1b) acquiring a channel key associated with a channel, (1c) wherein the channel comprises a plurality of virtual links through the public network that connects a plurality of channel nodes, the channel nodes including the source node and the destination node, such that only the channel nodes can communicate over the channel.

(2) sending the packet over a channel to the destination node using the address mapping, the address mapping reflecting a relationship between (a) an internal address for the destination node for use in communicating among nodes in the second private network and (b) an external address for the destination node suitable for communicating over the public network.

In Arrow, the determination of the source and destination of a transmitting packet is made with reference to Lookup Tables. Therefore, when a Lookup Result (LUR) for transmitting packet from the LookUp Tables maintain by the VPN unit is obtained, the LUR should correspond to a destination of the VPN unit 145-fig.1, see column 7, lines 28-32 (corresponding to (1a))

Arrow further discloses the VPN unit 115-fig.1 sending a received data packet to the VPN unit 145-fig.1 using the LUR, see column 7, line 46-column 8, line 20 (corresponding to (2)). The LUR reflects a relationship between an internal address for the destination node VPN unit 145-fig.1 in the Virtual Private Network for communication among the VPN units, see column 7, lines 28-32 (corresponding to (2a)), and an external address for the destination node VPN unit 145-fig.1 for communication over the public network, see column 11, lines 28-32 (corresponding to (2b)).

Arrow does disclose *forwarding the packet over a channel to a destination node* (remote client 140 of the VPN unit 145 -fig.1, Arrow) *in the second private network* (of the VPN group, see step 22-fig.2, Arrow) *based on the determination* (see column 8,

lines 18-19, Arrow), except acquiring a channel key associated with a channel base on the determination, *wherein the channel comprises a plurality of virtual links through the public network that connects a plurality of channel nodes, the channel nodes including the source node and the destination node, such that only the channel nodes are permitted to communicate over the channel*, wherein the channel key is updated for a modification of the channel nodes

However, in the same field of endeavor, Giniger discloses *forwarding the packet over a channel (secured tunneling) to a destination node (device 120-fig.1) in the second private network (VPN group, see col.7, lines 59-61) based on the determination by obtaining an address mapping corresponding to a destination node in the second network (see column 7, lines 54-64), and acquiring a channel key associated with a channel based on the determination (col.8, lines 28-42) wherein the channel comprises a plurality of virtual links (115-fig.1) through the public network that connects a plurality of channel nodes, the channel nodes including the source node and the destination node, such that only the channel nodes are permitted to communicate over the channel, wherein the channel key is updated for modification of the channel nodes (col.7, lines 44-67)*.

Therefore, it would have been obvious to an artisan to apply Giniger's teaching to Arrow's system with the motivation being to provide a secured data transmission between nodes over Internet and to prevent unauthenticated entering the VPN.

Regarding claim 8, Arrow (6,175,917) discloses A Method and Apparatus for Swapping A Computer Operating System. In Arrow, *a method for communicating between a first private network (LAN 110-fig.1) and a second private network (a VPN group including VPN units 115, 125, 135, 145, 155-fig.1, col.2, lines 22-27) that uses a public network infrastructure (public network 100-fig.1), comprising:*

receiving (receiving at VPN unit 145-fig.1) a packet from a source node (remote node 140-fig.1) in the second private network (VPN group-fig.1), (see column 8, lines 21-26);

determining (by the VPN unit 145-fig.1) whether the packet (from the remote node 140-fig.1) is destined for the second private network (in the VPN group, fig.1), (see column 8, lines 28-32)

Arrow does disclose *forwarding the packet over a channel to a destination node (remote client 140 of the VPN unit 145 -fig.1, Arrow) in the second private network (of the VPN group, see step 22-fig.2, Arrow) based on the determination (see column 8, lines 18-19, Arrow), except acquiring a channel key associated with a channel base on the determination, wherein the channel comprises a plurality of virtual links through the public network that connects a plurality of channel nodes, the channel nodes including the source node and the destination node, such that only the channel nodes are permitted to communicate over the channel, wherein the channel key is updated for a modification of the channel nodes*

However, in the same field of endeavor, Giniger discloses *forwarding the packet over a channel (secured tunneling) to a destination node (device 120-fig.1) in the second private network (VPN group, see col.7, lines 59-61) based on the determination by obtaining an address mapping corresponding to a destination node in the second network (see column 7, lines 54-64), and acquiring a channel key associated with a channel based on the determination (col.8, lines 28-42) wherein the channel comprises a plurality of virtual links (115-fig.1) through the public network that connects a plurality of channel nodes, the channel nodes including the source node and the destination node, such that only the channel nodes are permitted to communicate over the channel, wherein the channel key is updated for modification of the channel nodes (col.7, lines 44-67).*

Therefore, it would have been obvious to an artisan to apply Giniger's teaching to Arrow's system with the motivation being to provide a secured data transmission between nodes over Internet and to prevent unauthenticated entering the VPN.

Regarding claim 9, Arrow further discloses *said forwarding comprising:*

- (1) *sending the packet to the router node using the address mapping, wherein*
(a) the router node forwards the packet to the destination node based on an internal address in the packet for the destination node suitable for communicating among nodes in the first private network.

Arrow further discloses the VPN unit 145-fig.1 sending the received data packet from the node 140 to the VPN unit 115-fig.1 (*a router node*) using the LUR, see column 8, lines 21-32 (corresponding to (1)). The VPN unit 115-fig.1 (*the router node*) forwards the packet received from the VPN unit 145-fig.1 based on an internal address reflected from the LUR for the destination node 112-fig.1 in the LAN 110-fig.1 (*first private network*) for communication among the nodes 111 & 113, see column 6, lines 8-18; column 8, lines 42-52 (corresponding to (a)).

Regarding claim 10, The limitation of this claim calls for a packet transmission from a source 140-fig.1 to destination 112-fig.1, which is a reversed process of claim 3. Therefore, a data packet sending from a remote station 140-fig.1 should be encapsulated (corresponding to *adding the external address to the packet*) for transmission over the public network 100-fig.1 to destination 112-fig.1 via the VPN unit 145, 115, respectively, see column 7, lines 20-25.

Regarding claim 11, Arrow further discloses the VPN unit 145-fig.1 *encrypting the packet* in sending process from a source address 140-fig.1 to a destination address 112-fig.1 of the VPN unit 115-fig.1 in the VPN, see column 7, lines 46-50; column 6, lines 61-67.

Regarding claim 12, Arrow discloses the VPN unit 145-fig.1 accessing the LUR of a transmitting packet from the LookUp Tables maintaining by the VPN unit. If the LUR of the transmitting packet does not reflect a destination address 112-fig.1, then the transmitting packet from the node 140-fig.1 is not destined for the VPN unit 115-fig.1 to reach the unit 112-fig.1, see claim 8, also see also column 8, lines 29-33 (corresponding to *accessing the address mapping based on a determination that the packet is not destined for the second private network*).

Regarding claim 13, Arrow discloses the VPN unit 145-fig.1 accessing the Lookup Tables to obtain the LUR for a destination address in the transmitting packet. This LUR identifies the existence of a member of individual VPN, which corresponds to a destination 112-fig.1 of the VPN unit 115-fig.1, see claim 9, also see column 8, lines 26-32, (corresponding to *determining whether an address mapping exists for a destination address in the packet*).

Regarding claim 14:

Arrow (6,175,917) discloses A Method and Apparatus for Swapping A Computer Operating System. In Arrow, a *method for communicating between a first private network (LAN 110-fig.1) and a second private network (a VPN group including VPN*

units 115, 125, 135, 145, 155-fig.1, col.2, lines 22-27) that uses a public network infrastructure (public network 100-fig.1), comprising:

receiving (receiving at VPN unit 145-fig.1) a packet from a source node (remote node 140-fig.1) in the second private network (VPN group-fig.1), (see column 8, lines 21-26);

determining (by the VPN unit 145-fig.1) whether the packet (from the remote node 140-fig.1) is destined for the second private network (in the VPN group, fig.1), (see column 8, lines 28-32); and

In Arrow, the determination of the source and destination of a transmitting packet is made with reference to Lookup Tables. Therefore, when a Lookup Result (LUR) for the transmitting packet from the LookUp Tables maintain by the VPN unit is obtained, the LUR should correspond to a destination of the VPN unit 115-fig.1, (*a router node*), see column 8, lines 26-32 (corresponding to *obtaining an address mapping corresponding to a router node based on the determination*).

Arrow further discloses the VPN unit 145-fig.1 sending a received data packet to the VPN unit 115-fig.1 (*a router node*) using the LUR, see column 8, lines 21-32 (corresponding to *sending the packet over a channel to the router node using the address mapping*). The VPN unit 115-fig.1 (*the router node*) forwards the packet received from the VPN unit 145-fig.1 based on an internal address reflected from the LUR for the destination node 112-fig.1 in the LAN 110-fig.1 (*first private network*) for communication among the nodes 111 & 113, see column 6, lines 8-18; column 8, lines

42-52 (corresponding to *the router node forwards the packet to the destination node in the first private network based on an internal address in the packet for the destination node suitable for communicating among nodes in the first private network*)

Arrow does disclose *forwarding the packet over a channel to a destination node* (remote client 140 of the VPN unit 145 -fig.1, Arrow) *in the second private network* (of the VPN group, see step 22-fig.2, Arrow) *based on the determination* (see column 8, lines 18-19, Arrow), except acquiring a channel key associated with a channel base on the determination, *wherein the channel comprises a plurality of virtual links through the public network that connects a plurality of channel nodes, the channel nodes including the source node and the destination node, such that only the channel nodes are permitted to communicate over the channel*, wherein the channel key is updated for a modification of the channel nodes

However, in the same field of endeavor, Giniger discloses *forwarding the packet over a channel* (secured tunneling) *to a destination node* (device 120-fig.1) *in the second private network* (VPN group, see col.7, lines 59-61) *based on the determination by obtaining an address mapping corresponding to a destination node in the second network* (see column 7, lines 54-64), *and acquiring a channel key associated with a channel based on the determination* (col.8, lines 28-42) *wherein the channel comprises a plurality of virtual links* (115-fig.1) *through the public network that connects a plurality of channel nodes, the channel nodes including the source node and the destination node, such that only the channel nodes are permitted to communicate over the channel*,

wherein the channel key is updated for modification of the channel nodes (col.7, lines 44-67).

Therefore, it would have been obvious to an artisan to apply Giniger's teaching to Arrow's system with the motivation being to provide a secured data transmission between nodes over Internet and to prevent unauthenticated entering the VPN.

Regarding claim 15, Arrow discloses A Method and Apparatus for Swapping A Computer Operating System. In Arrow, *an apparatus* (VPN unit 115-fig.1 & also see fig.4) *for communicating between a first private network* (a LAN 110-fig.1) *and a second private network* (a VPN group including VPN units 115, 125, 135, 145, 155 in fig.1, col.2, lines 22-27) *that uses a public network infrastructure* (public network 100-fig.1), *comprising:*

a memory (a RAM 402-fig.4) *having program instructions* (instructions), see column 8, lines 59-60; *and*

a processor (a processor 400-fig.4) *responsive to* (for executing) *the program instructions* (instructions stored in the RAM 402-fig.4) *to receive a packet from a source node* (a node 112-fig.1) *in the first private network* (a LAN 110-fig.1), *determine whether the packet is destined for the second private network* (the VPN group, fig.1) *and forward the packet over a channel to a destination node* (a remote client 140-fig.1) *in the second private network based on the determination* (a processor 400-fig.4 receives a

transmitting packet from a source node 112-fig.1 in the LAN 110-fig.1. The processor 400-fig.4 determines whether the transmitting packet is destined for the VPN unit 145-fig.1 in the VPN group-fig.1, and forwards the transmitting packet to a destination node 140-fig.1 of the VPN unit 145 in the VPN group, see column 7, lines 20-48; see column 8, lines 18-19; and also see claim 1).

*Arrow does explicitly disclose *forwarding the packet over a channel to a destination node* (remote client 140 of the VPN unit 145 -fig.1, Arrow) *in the second private network* (of the VPN group, see step 22-fig.2, Arrow) *based on the determination* (see column 8, lines 18-19, Arrow), except acquire a channel key associated with a channel based on the determination, *wherein the channel comprises a plurality of virtual links through the public network that connects a plurality of channel nodes, the channel nodes including the source node and the destination node, such that only the channel nodes are permitted to communicate over the channel, wherein the channel key is updated for a modification of the channel nodes.**

*However, in the same field of endeavor, Giniger discloses *forwarding the packet over a channel* (secured tunneling) *to a destination node* (device 120-fig.1) *in the second private network* (VPN group, see col.7, lines 59-61) *based on the determination by obtaining an address mapping corresponding to a destination node in the second network* (see column 7, lines 54-64), and acquiring a channel key associated with a channel based on the determination (col.8, lines 28-42) *wherein the channel comprises a plurality of virtual links* (115-fig.1) *through the public network that connects a plurality**

of channel nodes, the channel nodes including the source node and the destination node, such that only the channel nodes are permitted to communicate over the channel, wherein the channel key is updated for modification of the channel nodes (col.7, lines 44-67).

Therefore, it would have been obvious to an artisan to apply Giniger's teaching to Arrow's system with the motivation being to provide a secured data transmission between nodes over Internet and to prevent unauthenticated entering the VPN.

Regarding claim 16, Arrow discloses A Method and Apparatus for Swapping A Computer Operating System. In Arrow, *an apparatus* (a VPN unit 145-fig.1 & also see fig.4) *for communicating between a first private network* (a LAN 110-fig.1) *and a second private network* (a VPN group including VPN units 115, 125, 135, 145, 155, fig.1, col.2, lines 22-27) *that uses a public network infrastructure* (public network 100-fig.1), *comprising:*

a memory (a RAM 402-fig.4) *having program instructions* (instructions), see column 8, lines 59-60; *and*

a processor (a processor 400-fig.4) *responsive to* (for executing) *the program instructions* (instructions stored in the RAM 402-fig.4) *to receive a packet from a source node* (a remote client 140-fig.1) *in the second private network* (the VPN group, fig.1), *determine whether the packet is destined for the second private network* (the VPN

group, fig.1), and forward the packet over a channel to a destination node (node 112-fig.1) in the first private network (LAN 110) based on the determination (a processor 400-fig.4 receives a transmitting packet from a source node 140-fig.1 of the VPN unit 145-fig.1 in the VPN group-fig.1. The processor 400-fig.4 determines whether the transmitting packet is destined for the VPN unit 115-fig.1 in the VPN group-fig.1, and forward the transmitting packet to a destination node 112-fig.1 of the VPN unit 115 in the VPN group, see column 8, lines 24-51. see column 6, lines 8-14, and also see claim 8).

Arrow does explicitly disclose *forwarding the packet over a channel to a destination node* (remote client 140 of the VPN unit 145 -fig.1, Arrow) *in the second private network* (of the VPN group, see step 22-fig.2, Arrow) *based on the determination* (see column 8, lines 18-19, Arrow), except acquire a channel key associated with a channel based on the determination, *wherein the channel comprises a plurality of virtual links through the public network that connects a plurality of channel nodes, the channel nodes including the source node and the destination node, such that only the channel nodes are permitted to communicate over the channel*, wherein the channel key is updated for a modification of the channel nodes.

However, in the same field of endeavor, Giniger discloses *forwarding the packet over a channel* (secured tunneling) *to a destination node* (device 120-fig.1) *in the second private network* (VPN group, see col.7, lines 59-61) *based on the determination by obtaining an address mapping corresponding to a destination node in the second*

network (see column 7, lines 54-64), and acquiring a channel key associated with a channel based on the determination (col.8, lines 28-42) wherein the channel comprises a plurality of virtual links (115-fig.1) through the public network that connects a plurality of channel nodes, the channel nodes including the source node and the destination node, such that only the channel nodes are permitted to communicate over the channel, wherein the channel key is updated for modification of the channel nodes (col.7, lines 44-67).

Therefore, it would have been obvious to an artisan to apply Giniger's teaching to Arrow's system with the motivation being to provide a secured data transmission between nodes over Internet and to prevent unauthenticated entering the VPN.

Regarding claim 17, Arrow (6,175,917) discloses A Method and Apparatus for Swapping A Computer Operating System. In Arrow, a *computer-readable medium* (a RAM 400-fig.4) *containing instructions for performing a method for communicating between a first private network (LAN 110-fig.1) and a second private network (a VPN group including VPN units 115, 125, 135, 145, 155-fig.1, col.2, lines 22-27) configured from nodes (VPN units, fig.1) in a public network infrastructure* (public network 100-fig.1), *comprising:*

receiving (receiving at VPN unit 115-fig.1) a packet from a source node (node 112-fig.1) in the first private network (LAN 110-fig.1), see column 7, lines 20-25;

determining (by the VPN unit 115-fig.1) whether the packet (from node 112-fig.1) is destined for the second private network (in the VPN group, fig.1), see column 7, lines 28-48; and

(1a) obtaining an address mapping corresponding to the destination node based on the determination and (1b) acquiring a channel key associated with a channel, (1c) wherein the channel comprises a plurality of virtual links through the public network that connects a plurality of channel nodes, the channel nodes including the source node and the destination node, such that only the channel nodes are permitted to communicate over the channel, and wherein the channel key is updated for a modification of the channel nodes.

(2) sending the packet over a channel to the destination node using the address mapping, the address mapping reflecting a relationship between (a) an internal address for the destination node for use in communicating among nodes in the second private network and (b) an external address for the destination node suitable for communicating over the public network,

In Arrow, the determination of the source and destination of a transmitting packet is made with reference to Lookup Tables. Therefore, when a Lookup Result (LUR) for transmitting packet from the LookUp Tables maintain by the VPN unit is obtained, the LUR should correspond to a destination of the VPN unit 145-fig.1, see column 7, lines 28-32 (corresponding to (1))

Arrow further discloses the VPN unit 115-fig.1 sending a received data packet to the VPN unit 145-fig.1 using the LUR, see column 7, line 46-column 8, line 20 (corresponding to (2)). The LUR reflects a relationship between an internal address for the destination node VPN unit 145-fig.1 in the Virtual Private Network for communication among the VPN units, see column 7, lines 28-32 (corresponding to (a)), and an external address for the destination node VPN unit 145-fig.1 for communication over the public network, see column 11, lines 28-32 (corresponding to (b)).

Arrow does explicitly disclose *forwarding the packet over a channel to a destination node* (remote client 140 of the VPN unit 145 -fig.1, Arrow) *in the second private network* (of the VPN group, see step 22-fig.2, Arrow) *based on the determination* (see column 8, lines 18-19, Arrow), except (1b) acquiring a channel key associated with a channel based on the determination, (1c) *wherein the channel comprises a plurality of virtual links through the public network that connects a plurality of channel nodes, the channel nodes including the source node and the destination node, such that only the channel nodes are permitted to communicate over the channel*, and wherein the channel key is updated for a modification of the channel nodes.

However, in the same field of endeavor, Giniger discloses *forwarding the packet over a channel* (secured tunneling) to a *destination node* (device 120-fig.1) *in the second private network* (VPN group, see col.7, lines 59-61) *based on the determination by obtaining an address mapping corresponding to a destination node in the second network* (see column 7, lines 54-64), and acquiring a channel key associated with a

channel based on the determination (col.8, lines 28-42) wherein the channel comprises a plurality of virtual links (115-fig.1) through the public network that connects a plurality of channel nodes, the channel nodes including the source node and the destination node, such that only the channel nodes are permitted to communicate over the channel, wherein the channel key is updated for modification of the channel nodes (col.7, lines 44-67).

Therefore, it would have been obvious to an artisan to apply Giniger's teaching to Arrow's system with the motivation being to provide a secured data transmission between nodes over Internet and to prevent unauthenticated entering the VPN.

Regarding claim 18, Arrow discloses when the data packet sending from an end-station 112-fig.1 to a router 114-fig.1, the packet is encapsulated (corresponding to *adding external address*) for transmission to a destination node 140 in the VPN unit 145-fig.1 in the public network 100-fig.1 through the VPN unit 115, see column 7, lines 20-25

Regarding claim 19, Arrow further discloses the VPN unit 115-fig.1 *encrypting the packet* in sending process from a source address 112-fig.1 to a destination address 140-fig.1 of VPN unit 145-fig.1 in the VPN, see column 7, line 46-column 8, line 20 & specific in column 7, lines 57-60; also see column 6, lines 61-67.

Regarding claim 20, Arrow further discloses the VPN unit 115-fig.1 accessing the LUR of the transmitting packet from the Lookup Tables. This LUR should correspond to a destination of the VPN unit 145-fig.1, see column 7, lines 28-32, also see claim 17, (corresponding to *accessing the address mapping based on a determination that the packet is destined for the second private network*).

Regarding claim 21 Arrow further discloses the VPN unit 115-fig.1 accessing the Lookup Tables to obtain a LUR for a destination address in the transmitting packet. This LUR identifies the existence of a member of individual VPN, which corresponds to the destination 140-fig.1 via the VPN unit 145-fig.1, see column 7, lines 28-32, 50-52, also see claim 17, (corresponding to *determining whether an address mapping exists for a destination address in the packet*).

Regarding claim 22, Arrow (6,175,917) discloses A Method and Apparatus for Swapping A Computer Operating System. In Arrow, a *computer-readable medium* (a RAM 400-fig.4) *containing instructions for performing a method for communicating between a first private network (LAN 110-fig.1) and a second private network (a VPN group including VPN units 115, 125, 135, 145, 155-fig.1, col.2, lines 22-27) configured*

from nodes (VPN units, fig.1) in a public network infrastructure (public network 100-fig.1), comprising:

receiving (receiving at VPN unit 145-fig.1) a packet from a source node (remote node 140-fig.1) in the second private network (VPN group-fig.1), see column 8, lines 21-26;

determining (by the VPN unit 145-fig.1) whether the packet (from the remote node 140-fig.1) is destined for the second private network (in the VPN group, fig.1), see column 8, lines 28-32; and

(1) obtaining an address mapping corresponding to a router node and acquiring a channel key associated with a channel based on the determination, wherein the channel comprises a plurality of virtual links through the public network that connects a plurality of channel nodes, the channel nodes including the source node and the destination node, such that only the channel nodes are permitted to communicate over the channel, wherein the channel key is updated for a modification of the channel nodes;

(2) sending the packet over a channel to the router node using the address mapping, wherein the router node forwards the packet to a destination node in the first private network based on an internal address in the packet for the destination node suitable for communicating among nodes in the first private network.

In Arrow, the determination of the source and destination of a transmitting packet is made with reference to Lookup Tables. Therefore, when a Lookup Result (LUR) for

Art Unit: 2665

transmitting packet from the LookUp Tables maintain by the VPN unit is obtained, the LUR should correspond to a destination of the VPN unit 115-fig.1, see column 8, lines 26-32 (corresponding to (1)).

Arrow further discloses the VPN unit 145-fig.1 sending the received data packet from the node 140 to the VPN unit 115-fig.1 (*a router node*) using the LUR, see column 8, lines 21-32 (corresponding to (2)). The VPN unit 115-fig.1 (*the router node*) forwards the packet received from the VPN unit 145-fig.1 based on an internal address reflected from the LUR for the destination node 112-fig.1 in the LAN 110-fig.1 (*first private network*) for communication among the nodes 111 & 113, see column 6, lines 8-18; column 8, lines 42-52 (corresponding to (a)).

Arrow does disclose *forwarding the packet over a channel to a destination node* (remote client 140 of the VPN unit 145 -fig.1, Arrow) *in the second private network* (of the VPN group, see step 22-fig.2, Arrow) *based on the determination* (see column 8, lines 18-19, Arrow), except acquiring a channel key associated with a channel base on the determination, *wherein the channel comprises a plurality of virtual links through the public network that connects a plurality of channel nodes, the channel nodes including the source node and the destination node, such that only the channel nodes are permitted to communicate over the channel*, wherein the channel key is updated for a modification of the channel nodes.

However, in the same field of endeavor, Giniger discloses *forwarding the packet over a channel* (secured tunneling) *to a destination node* (device 120-fig.1) *in the*

second private network (VPN group, see col.7, lines 59-61) based on the determination by obtaining an address mapping corresponding to a destination node in the second network (see column 7, lines 54-64), and acquiring a channel key associated with a channel based on the determination (col.8, lines 28-42) wherein the channel comprises a plurality of virtual links (115-fig.1) through the public network that connects a plurality of channel nodes, the channel nodes including the source node and the destination node, such that only the channel nodes are permitted to communicate over the channel, wherein the channel key is updated for modification of the channel nodes (col.7, lines 44-67).

Therefore, it would have been obvious to an artisan to apply Giniger's teaching to Arrow's system with the motivation being to provide a secured data transmission between nodes over Internet and to prevent unauthenticated entering the VPN.

Regarding claim 23, The limitation of this claim calls for a packet transmission from a source 140-fig.1 to destination 112-fig.1, which is a reversed process of claim 3. Therefore, a data packet sending from a remote station 140-fig.1 should be encapsulated (corresponding to *adding the external address to the packet*) for transmission over the public network 100-fig.1 to destination 112-fig.1 via the VPN unit 145, 115, respectively, see column 7, lines 20-25.

Regarding claim 24, Arrow further discloses the VPN unit 145-fig.1 *encrypting the packet* in sending process from a source address 140-fig.1 to a destination address 112-fig.1 of the VPN unit 115-fig.1 in the VPN, see column 7, lines 46-50; column 6, lines 61-67.

Regarding claim 25, Arrow discloses the VPN unit 145-fig.1 accessing the LUR of a transmitting packet from the LookUp Tables maintaining by the VPN unit. If the LUR of the transmitting packet does not reflect a destination address 112-fig.1, then the transmitting packet from the node 140-fig.1 is not destined for the VPN unit 115-fig.1 to reach the unit 112-fig.1, see also column 8, lines 29-33, and also see claim 22, (corresponding to *accessing the address mapping based on a determination that the packet is not destined for the second private network*).

Regarding claim 26, Arrow discloses the VPN unit 145-fig.1 accessing the Lookup Tables to obtain the LUR for a destination address in the transmitting packet. This LUR identifies the existence of a member of individual VPN, which corresponds to a destination 112-fig.1 of the VPN unit 115-fig.1, see claim 9, also see column 8, lines 26-32, also see claim 22, (corresponding to *determining whether an address mapping exists for a destination address in the packet*).

Regarding claim 27, Arrow (6,175,917) discloses A Method and Apparatus for Swapping A Computer Operating System. In Arrow, *a method for communicating between a first private network (LAN 110-fig.1) and a second private network (a VPN group including VPN units 115, 125, 135, 145, 155-fig.1, col.2, lines 22-27) configured from nodes (VPN units, fig.1) in a public network infrastructure (public network 100-fig.1), comprising:*

means for receiving (VPN unit 115-fig.1) a packet from a source node (node 112-fig.1) in the first private network (LAN 110-fig.1), see column 7, lines 20-25;

means for determining (by the VPN unit 115-fig.1) whether the packet (from node 112-fig.1) is destined for the second private network (in the VPN group, fig.1), see column 7, lines 28-48;

(1) means for obtaining an address mapping corresponding to the destination node and acquiring a channel key associated with a channel based on the determination; and

(2) means for sending the packet over a channel to the destination node using the address mapping, the address mapping reflecting a relationship between (a) an internal address for the destination node for use in communicating among nodes in the second private network and (b) an external address for the destination node suitable for communicating over the public network infrastructure.

In Arrow, the determination of the source and destination of a transmitting packet is made with reference to Lookup Tables. Therefore, when a Lookup Result (LUR) for transmitting packet from the LookUp Tables maintain by the VPN unit is obtained, the LUR should correspond to a destination of the VPN unit 145-fig.1, see column 7, lines 28-32 (corresponding to (1)).

Arrow further discloses the VPN unit 115-fig.1 sending a received data packet to the VPN unit 145-fig.1 using the LUR, see column 7, line 46-column 8, line 20 (corresponding to (2)). The LUR reflects a relationship between an internal address for the destination node VPN unit 145-fig.1 in the Virtual Private Network for communication among the VPN units, see column 7, lines 28-32 (corresponding to (a)), and an external address for the destination node VPN unit 145-fig.1 for communication over the public network, see column 7, lines 28-32 (corresponding to (b)).

Arrow does disclose *forwarding the packet over a channel to a destination node* (remote client 140 of the VPN unit 145 -fig.1, Arrow) *in the second private network* (of the VPN group, see step 22-fig.2, Arrow) *based on the determination* (see column 8, lines 18-19, Arrow), except acquiring a channel key associated with a channel base on the determination.

However, in the same field of endeavor, Giniger discloses *forwarding the packet over a channel* (secured tunneling) *to a destination node* (device 120-fig.1) *in the second private network* (VPN group, see col.7, lines 59-61) *based on the determination by obtaining an address mapping corresponding to a destination node in the second*

network (see column 7, lines 54-64), and acquiring a channel key associated with a channel based on the determination (col.8, lines 28-42).

Therefore, it would have been obvious to an artisan to apply Giniger's teaching to Arrow's system with the motivation being to provide a secured data transmission between nodes over Internet and to prevent unauthenticated entering the VPN.

Regarding claim 28, Arrow discloses when the data packet sending from an end-station 112-fig.1 to a router 114-fig.1, the packet is encapsulated (corresponding to *adding external address*) for transmission to a destination node 140 in the VPN unit 145-fig.1 in the public network 100-fig.1 through the VPN unit 115, see column 7, lines 20-25.

Regarding claim 29, Arrow further discloses the VPN unit 115-fig.1 *encrypting the packet* in sending process from a source address 112-fig.1 to a destination address 140-fig.1 of VPN unit 145-fig.1 in the VPN, see column 7, line 46-column 8, line 20 & in specific column 7, lines 57-60.

Regarding claim 30, Arrow further discloses the VPN unit 115-fig.1 accessing the LUR of the transmitting packet from the Lookup Tables. This LUR should correspond to a

destination of the VPN unit 145-fig.1, see column 7, lines 28-32, also see claim 27, (corresponding to *means for accessing the address mapping based on a determination that the packet is destined for the second private network*).

Regarding claim 31, Arrow further discloses the VPN unit 115-fig.1 accessing the Lookup Tables to obtain a LUR for a destination address in the transmitting packet. This LUR identifies the existence of a member of individual VPN, which corresponds to the destination 140-fig.1 via the VPN unit 145-fig.1, see column 7, lines 28-32, 50-52, also see claim 27, (corresponding to *determining whether an address mapping exists for a destination address in the packet*).

Regarding claim 32:

Arrow (6,175,917) discloses A Method and Apparatus for Swapping A Computer Operating System. In Arrow, *an apparatus* (VPN unit 145-fig.1) *for communicating between a first private network (LAN 110-fig.1) and a second private network (a VPN group including VPN units 115, 125, 135, 145, 155-fig.1, col.2, lines 22-27) configured from nodes (VPN units, fig.1) in a public network infrastructure* (public network 100-fig.1), *comprising*:

means for receiving (VPN unit 145-fig.1) a packet from a source node (remote node 140-fig.1) in the second private network (VPN group-fig.1), see column 8, lines 21-26;

means for determining (by the VPN unit 145-fig.1) whether the packet (from the remote node 140-fig.1) is destined for the second private network (in the VPN group, fig.1), see column 8, lines 28-32; and

(1) means for obtaining an address mapping corresponding to a router node and acquiring a channel key associated with a channel based on the determination;

(2) means for sending the packet to the router node using the address mapping,
(a) wherein the router node forwards the packet to a destination node in the first private network based on an internal address in the packet for the destination node suitable for communicating among nodes in the first private network,

In Arrow, the determination of the source and destination of a transmitting packet is made with reference to Lookup Tables. Therefore, when a Lookup Result (LUR) for transmitting packet from the LookUp Tables maintain by the VPN unit is obtained, the LUR should correspond to a destination of the VPN unit 115-fig.1, , see column 8, lines 26-32 (corresponding to (1)).

Arrow further discloses the VPN unit 145-fig.1 sending the received data packet from the node 140 to the VPN unit 115-fig.1 (*a router node*) using the LUR, see column 8, lines 21-32 (corresponding to (2)). The VPN unit 115-fig.1 (*the router node*) forwards

the packet received from the VPN unit 145-fig.1 based on an internal address reflected from the LUR for the destination node 112-fig.1 in the LAN 110-fig.1 (*first private network*) for communication among the nodes 111 & 113, see column 6, lines 8-18; column 8, lines 42-52 (corresponding to (a)).

Arrow does explicitly disclose *forwarding the packet over a channel to a destination node* (remote client 140 of the VPN unit 145 -fig.1, Arrow) *in the second private network* (of the VPN group, see step 22-fig.2, Arrow) *based on the determination* (see column 8, lines 18-19, Arrow), except acquiring a channel key associated with a channel base on the determination.

However, in the same field of endeavor, Giniger discloses *forwarding the packet over a channel* (secured tunneling) *to a destination node* (device 120-fig.1) *in the second private network* (VPN group, see col.7, lines 59-61) *based on the determination by obtaining an address mapping corresponding to a destination node in the second network* (see column 7, lines 54-64), *and acquiring a channel key associated with a channel based on the determination* (col.8, lines 28-42).

Therefore, it would have been obvious to an artisan to apply Giniger's teaching to Arrow's system with the motivation being to provide a secured data transmission between nodes over Internet and to prevent unauthenticated entering the VPN.

Regarding claim 33, The limitation of this claim calls for a packet transmission from a source 140-fig.1 to destination 112-fig.1, which is a reversed process of claim 27. Therefore, a data packet sending from a remote station 140-fig.1 should be encapsulated (corresponding to *adding the external address to the packet*) for transmission over the public network 100-fig.1 to destination 112-fig.1 via the VPN unit 145, 115, respectively, see column 7, lines 20-25.

Regarding claim 34, Arrow further discloses the VPN unit 145-fig.1 *encrypting the packet* in sending process from a source address 140-fig.1 to a destination address 112-fig.1 of the VPN unit 115-fig.1 in the VPN, see column 7, lines 46-50; column 6, lines 61-67.

Regarding claim 35, Arrow discloses the VPN unit 145-fig.1 accessing the LUR of a transmitting packet from the LookUp Tables maintaining by the VPN unit. If the LUR of the transmitting packet does not reflect a destination address 112-fig.1, then the transmitting packet from the node 140-fig.1 is not destined for the VPN unit 115-fig.1 to reach the unit 112-fig.1, see claim 8, also see also column 8, lines 29-33 (corresponding to *accessing the address mapping based on a determination that the packet is not destined for the second private network*).

Regarding claim 36, Arrow discloses the VPN unit 145-fig.1 accessing the Lookup Tables to obtain the LUR for a destination address in the transmitting packet. This LUR identifies the existence of a member of individual VPN, which corresponds to a destination 112-fig.1 of the VPN unit 115-fig.1, see claim 9, also see column 8, lines 26-32, (corresponding to *determining whether an address mapping exists for a destination address in the packet*).

Regarding claim 37, Arrow (6,175,917) discloses A Method and Apparatus for Swapping A Computer Operating System. In Arrow, a *method for communicating between a first private network (LAN 110-fig.1) and a second private network (a VPN group including VPN units 115, 125, 135, 145, 155-fig.1, col.2, lines 22-27) configured from nodes (VPN units, fig.1) in a public network (public network 100-fig.1), comprising:*

receiving, at VPN unit 115-fig.1, a first packet from a source node (node 112-fig.1) in the first private network (LAN 110-fig.1), see column 7, lines 20-25, wherein the router node (VPN unit 115-fig.1) facilitates connection between the first private network (the LAN 110-fig.1) and the second private network (the VPN group-fig.1)

determining (by the VPN unit 115-fig.1) whether the first packet (from node 112-fig.1) is destined for the second private network (VPN unit 145 in the VPN group, fig.1), see column 7, lines 28-48;

(1a) obtaining an address mapping corresponding to a second destination node and (1b) acquiring a channel key associated with a channel based on the determination and (1c) wherein the channel comprises a plurality of virtual links through the public network that connects a plurality of channel nodes, the channel nodes including the source node and the destination node, such that only the channel nodes can communicate over the channel.

(2) sending the packet over a channel to the second destination node using the address mapping, the address mapping reflecting a relationship between (2a) an internal address for the second destination node for use in communicating among nodes in the second private network and (2b) an external address for the second destination node suitable for communicating over the public infrastructure,

In Arrow, the determination of the source and destination of a transmitting packet is made with reference to Lookup Tables. Therefore, when a Lookup Result (LUR) for transmitting packet from the LookUp Tables maintain by the VPN unit is obtained, the LUR should correspond to a destination of the VPN unit 145-fig.1, see column 7, lines 28-32 (corresponding to (1a)).

Arrow further discloses the VPN unit 115-fig.1 sending a received data packet to the VPN unit 145-fig.1 using the LUR, see column 7, line 46-column 8, line 20 (corresponding to (2)). The LUR reflects a relationship between an internal address for the destination node VPN unit 145-fig.1 in the Virtual Private Network for communication among the VPN units, see column 7, lines 28-32 (corresponding to

(2a)), and an external address for the destination node VPN unit 145-fig.1 for communication over the public network, see column 7, lines 28-32 (corresponding to (2b)).

receiving (receiving at VPN unit 145-fig.1) a second packet from a source node (remote node 140-fig.1) in the second private network (VPN group-fig.1), see column 8, lines 21-26;

determining (by the VPN unit 145-fig.1) whether the second packet (from the remote node 140-fig.1) is destined for the second private network (VPN unit 115 in the VPN group, fig.1), see column 8, lines 28-32; and

(3) obtaining an address mapping corresponding to the router node based on the determination that the second packet is not destined for the second private network;
and

(4) sending the packet over the channel to the router node using the address mapping corresponding to the router node, wherein (4a) the router node forwards the packet to the first destination node based on an internal address in the second packet for the first destination node suitable for communicating among nodes in the first private network.

In Arrow, the determination of the source and destination of a transmitting packet is made with reference to Lookup Tables. Therefore, when a Lookup Result (LUR) for transmitting packet from the LookUp Tables maintain by the VPN unit is obtained, the

LUR should correspond to a destination of the VPN unit 115-fig.1, see column 8, lines 26-33 (corresponding to (3)).

Arrow further discloses the VPN unit 145-fig.1 sending the received data packet from the node 140 to the VPN unit 115-fig.1 (*a router node*) using the LUR, see column 8, lines 21-32 (corresponding to (4)). The VPN unit 115-fig.1 (*the router node*) forwards the packet received from the VPN unit 145-fig.1 based on an internal address reflected from the LUR for the destination node 112-fig.1 in the LAN 110-fig.1 (*first private network*) for communication among the nodes 111 & 113, see column 6, lines 8-18; column 8, lines 21-52 (corresponding to (4a)).

Arrow does disclose *forwarding the packet over a channel to a destination node* (remote client 140 of the VPN unit 145 -fig.1, Arrow) *in the second private network* (of the VPN group, see step 22-fig.2, Arrow) *based on the determination* (see column 8, lines 18-19, Arrow), except acquiring a channel key associated with a channel base on the determination, *wherein the channel comprises a plurality of virtual links through the public network that connects a plurality of channel nodes, the channel nodes including the source node and the destination node, such that only the channel nodes are permitted to communicate over the channel*, wherein the channel key is updated for a modification of the channel nodes

However, in the same field of endeavor, Giniger discloses *forwarding the packet over a channel* (secured tunneling) *to a destination node* (device 120-fig.1) *in the second private network* (VPN group, see col.7, lines 59-61) *based on the determination*

by obtaining an address mapping corresponding to a destination node in the second network (see column 7, lines 54-64), and acquiring a channel key associated with a channel based on the determination (col.8, lines 28-42) wherein the channel comprises a plurality of virtual links (115-fig.1) through the public network that connects a plurality of channel nodes, the channel nodes including the source node and the destination node, such that only the channel nodes are permitted to communicate over the channel, wherein the channel key is updated for modification of the channel nodes (col.7, lines 44-67).

Therefore, it would have been obvious to an artisan to apply Giniger's teaching to Arrow's system with the motivation being to provide a secured data transmission between nodes over Internet and to prevent unauthenticated entering the VPN.

Response to Arguments

3. Applicant's arguments with respect to claims have been considered but are moot in view of the new ground(s) of rejection.

A/. Applicant argued that neither Giniger (6,751,729) or/and Arrow (6,175,917) disclose "acquiring a channel key associated with a channel based on the determination, wherein the channel comprises a plurality of virtual links through the public network that connects a plurality of channel nodes, the channel nodes including the source node and the destination node, such that only the channel nodes are

permitted to communicate over the channel, and wherein the channel key is updated for a modification of channel nodes".

In reply, applicant is directed to Giniger, column 8, lines 28-42, wherein edge nodes (source and destination nodes) are permitted to communicate over a secure communication tunnel (channel) using a session key assigned by the management server 130, the session key is used for selecting a particular tunnel that coupled to the edge nodes and passing the communication through the tunnel from a source node to its destination (see col.7, line 33-col.9, line 20). The session key is updated corresponding to the particular tunnel of edge nodes to secure the encrypting communication passing through the particular tunnel (channel).

4. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Phuongchau Ba Nguyen whose telephone number is 571-272-3148. The examiner can normally be reached on Monday-Friday from 10:00 a.m. to 2:00 p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Huy Vu can be reached on 571-272-3155. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Phuongchau Ba Nguyen
Examiner
Art Unit 2665

DUC HO
PRIMARY EXAMINER


D2-06-06